

EMBEDDINGS OF FIELDS INTO SIMPLE ALGEBRAS: GENERALIZATIONS AND APPLICATIONS

CHIA-FU YU

ABSTRACT. For two semi-simple algebras A and B over an arbitrary ground field F , we give a numerical criterion when $\text{Hom}_{F\text{-alg}}(A, B)$, the set of F -algebra homomorphisms between them, is non-empty. We also determine when the orbit set $B^\times \setminus \text{Hom}_{F\text{-alg}}(A, B)$ is finite and give an explicit formula for its cardinality. A few applications of main results are given.

1. INTRODUCTION

Semi-simple algebras are the most fundamental objects in the non-commutative ring theory. They also serve as a useful tool for studying some basic objects in algebraic geometry and number theory such as abelian varieties, Drinfeld modules, or elliptic sheaves those form a semi-simple category. While studying objects X as above with extra symmetries, one considers objects X together with an additional structure $\iota : A \rightarrow \text{End}(X) \otimes \mathbb{Q}$ on X by a semi-simple algebra A . This leads to a general question when a homomorphism exists from a given semi-simple algebra to another one.

We let F denote the ground field. Suppose A is a (finite-dimensional) central simple algebra over F , and K a finite field extension of F . In what condition does there exist an F -algebra embedding of K into A ? The following well-known result answers this question; see [4, 13.3 Theorem and Corollary, p. 241].

Theorem 1.1. *Assume that $[K : F] = \sqrt{[A : F]}$. Then there is an embedding of K into A as F -algebras if and only if K splits A , i.e. $A \otimes_F K$ is a matrix algebra over K . In this case, K is isomorphic to a strictly maximal subfield of A .*

Note that any F -algebra homomorphism from K to A is an embedding. In this paper we consider the following general problem of embedding of a semi-simple algebra into another one:

(P1) Let A and B be two semi-simple F -algebras. Find a necessary and sufficient condition for them such that there is an embedding or a homomorphism of F -algebras from A into B .

Let $\text{Hom}_{F\text{-alg}}(A, B)$ denote the set of all F -algebra homomorphisms from A into B , and let $\text{Hom}_{F\text{-alg}}^*(A, B) \subset \text{Hom}_{F\text{-alg}}(A, B)$ denote the subset consisting of embeddings. Problem **(P1)** asks when the set $\text{Hom}_{F\text{-alg}}(A, B)$ or $\text{Hom}_{F\text{-alg}}^*(A, B)$

Date: January 21, 2013.

2000 Mathematics Subject Classification. 16R20, 11R52, 16K.

Key words and phrases. semi-simple algebras, embeddings, the local-global principle.

is non-empty. For an F -algebra A , denote by $\text{rad}(A)$ the Jacobson radical of A and $A^{ss} := A/\text{rad}(A)$ the maximal semi-simple quotient of A . Denote by A° the opposite algebra of A . If A is semi-simple, then one can write

$$A \simeq \prod_{i=1}^s \text{Mat}_{n_i}(D_i),$$

where D_i are division algebras over F , which is also called the Wedderburn decomposition of A .

One of our main theorems is the following, which solves Problem **(P1)**.

Theorem 1.2 (Theorem 2.5). *Let A and B be two semi-simple F -algebras. We realize B as $\prod_{j=1}^r \text{End}_{\Delta_j}(V_j)$, where Δ_j is a division F -algebra and V_j is a right Δ_j -module for each j . Write $A = \prod_{i=1}^s A_i$ into the product of simple F -algebras.*

(1) *For each j , write the maximal semi-simple quotient*

$$(\Delta_j \otimes_F A^\circ)^{ss} = \prod_{k=1}^{t_j} \text{Mat}_{m_{jk}}(D_{jk})$$

of $\Delta_j \otimes_F A^\circ$ as the product of simple factors (the Wedderburn decomposition). Then the set $\text{Hom}_{F\text{-alg}}(A, B)$ is non-empty if and only if there are non-negative integers x_{jk} for $j = 1, \dots, r$ and $k = 1, \dots, t_j$ such that

- (a) $\sum_{k=1}^{t_j} x_{jk} = \dim_{\Delta_j} V_j$ for all j , and
- (b) for all j, k , one has

$$\frac{m_{jk}[D_{jk} : F]}{[\Delta_j : F]} \Big| x_{jk}.$$

(2) *For each j, i , write the maximal semi-simple quotient*

$$(\Delta_j \otimes_F A_i^\circ)^{ss} = \prod_{k=1}^{t_{ji}} \text{Mat}_{m_{jik}}(D_{jik})$$

of $\Delta_j \otimes_F A_i^\circ$ as the product of simple factors. Then the set $\text{Hom}_{F\text{-alg}}^(A, B)$ is non-empty if and only if there are non-negative integers x_{jik} for $j = 1, \dots, r$, $i = 1, \dots, s$ and $k = 1, \dots, t_{ji}$ such that*

- (a) $\sum_{i,k} x_{jik} = \dim_{\Delta_j} V_j$ for all j ,
- (b) for all j, i, k , one has

$$\frac{m_{jik}[D_{jik} : F]}{[\Delta_j : F]} \Big| x_{jik}, \quad \text{and}$$

- (c) for all i , the sum $\sum_{j,k} x_{jik}$ is positive.

Theorem 1.2 provides a numerical criterion for the problem **(P1)**. However, it still looks technical. In the special case when B is a central simple algebra over F , the criterion in Theorem 1.2 can be simplified as follows (This form will be used for applications):

Theorem 1.3 (Theorem 2.7). *Let $B = \text{Mat}_n(\Delta)$ be a central simple algebra of F , where Δ is the division part of B . Let $A = \prod_{i=1}^s A_i$ be a semi-simple F -algebra and let K_i be the center of A_i for each i . Then there is an embedding from the F -algebra A into B if and only if there are positive integers n_i for $i = 1, \dots, s$ such that*

$$(1.1) \quad n = \sum_{i=1}^s n_i, \quad \text{and} \quad [A_i : F] \mid n_i c_i, \quad \forall i = 1, \dots, s,$$

where c_i the capacity of the central simple algebra $\Delta \otimes_F A_i^\circ$ over K_i .

Recall ([7, p. 179], also see Definition 2.6) that the *capacity* of a central simple algebra A is the number c so that $A \simeq \text{Mat}_c(D)$, where D is a division algebra, also called the division part of A .

The problem **(P1)** does not seem to be studied in this generality in the literature. The only related result we know was obtained by Chuard-Koulmann and Morales [1], who studied, among other things, the embeddability of a Frobenius algebra A into a central simple algebra B with the condition $[A : F] = \deg(B)$. The overlap with [1] is a consequence (Corollary 2.8) of Theorem 1.3 where A is a commutative étale F -algebra and $[A : F] = \deg(B)$ (and B is still central simple). Two approaches of studying embeddings of algebras are different. As we also need to deal with non-separable algebras, the method of Galois cohomology is not applicable in our situation.

The second part of this paper studies how many “essentially different” F -algebra homomorphisms there are from A into B . There are two natural notions of equivalence relations:

- (1) Two F -algebra homomorphisms $\varphi_1, \varphi_2 : A \rightarrow B$ are said to be *equivalent* if there is an element $b \in B^\times$ such that $\varphi_2 = \text{Int}(b) \circ \varphi_1$. That is, $\varphi_2(a) = b \varphi_1(a) b^{-1}$ for all $a \in A$.
- (2) Two F -algebra homomorphism $\varphi_1, \varphi_2 : A \rightarrow B$ are said to be *weakly equivalent* if there is an F -automorphism $\alpha \in \text{Aut}_F(B)$ of B such that $\varphi_2 = \alpha \circ \varphi_1$.

So the problem simply becomes asking for the size of the orbit set $B^\times \backslash \text{Hom}_{F\text{-alg}}(A, B)$ or the orbit set $\text{Aut}_F(B) \backslash \text{Hom}_{F\text{-alg}}(A, B)$, where the groups B^\times and $\text{Aut}_F(B)$ act naturally on the set $\text{Hom}_{F\text{-alg}}(A, B)$ from the left. In this paper we consider the equivalence relation defined in (1). Put

$$\mathcal{O}_{A,B} := B^\times \backslash \text{Hom}_{F\text{-alg}}(A, B).$$

(P2) Is the orbit set $\mathcal{O}_{A,B}$ finite? If so, then what is its cardinality $|\mathcal{O}_{A,B}|$?

Results toward this direction may be viewed as the generalization of the Noether-Skolem theorem. In [5] F. Pop and H. Pop showed that the orbit set $\mathcal{O}_{A,B}$ is finite when B is separable over F . Recall [7, p. 101] that an F -algebra is said to be *separable over F* if it is semi-simple and its center Z is étale over F , i.e. Z is a finite product of finite separable field extensions of F . The second main result of this paper solves the problem **(P2)** completely. The answer turns out to be negative in general; the finiteness of the orbit set is encoded in the Kähler modules of the center of $A \otimes_F B$. We give a necessary and sufficient condition for A and B so that the orbit set $\mathcal{O}_{A,B}$ is finite. In addition, we compute the precise number of $|\mathcal{O}_{A,B}|$ when A or B is separable over F (a upper bound for $|\mathcal{O}_{A,B}|$ is given in [5] when B is separable).

We now state the explicit result for $\mathcal{O}_{A,B}$. We may assume that B is simple; indeed if $B = \prod_{j=1}^r B_j$ is semi-simple, where B_j 's are simple factors, then one has

$\mathcal{O}_{A,B} = \prod_{j=1}^r \mathcal{O}_{A,B_j}$. Write $B = \text{Mat}_n(\Delta)$, where Δ is a division algebra over F . Write the maximal semi-simple quotient of $\Delta \otimes_F A^\circ$ into the product of simple factors:

$$(1.2) \quad (\Delta \otimes_F A^\circ)^{ss} \simeq \prod_{i=1}^t \text{Mat}_{m_i}(D_i),$$

where D_i is a division algebra. We show (Proposition 2.3) that the algebra $\Delta \otimes_F A^\circ$ has the following form

$$(1.3) \quad \Delta \otimes_F A^\circ \simeq \prod_{i=1}^t \text{Mat}_{m_i}(\tilde{D}_i),$$

where \tilde{D}_i is an Artinian F -algebra whose maximal semi-simple quotient is equal to D_i . Put $R_i := Z(\tilde{D}_i)$ and $Z_i := Z(D_i) = (R_i)^{ss}$. Let \mathfrak{m}_{R_i} be the maximal ideal of R_i ; one has $Z_i = R_i/\mathfrak{m}_{R_i}$. Since there is an embedding from Δ into $\text{Mat}_{m_i}(D_i)$, one has $[\Delta : F] \mid m_i[D_i : F]$. Put

$$(1.4) \quad \ell_i := m_i[D_i : F]/[\Delta : F] \in \mathbb{N},$$

and

$$(1.5) \quad P(A, B) := \{(x_1, \dots, x_t) \in \mathbb{Z}_{\geq 0}^t \mid \dim_{\Delta} V = \sum_{i=1}^t \ell_i x_i\}.$$

Theorem 1.4 (Theorem 3.6). *Let A be a semi-simple F -algebra and $B = \text{Mat}_n(\Delta)$ a simple F -algebra. Let $\tilde{D}_i, D_i, R_i, Z_i$ and $P(A, B)$ be as above.*

- (1) *The orbit set $\mathcal{O}_{A,B}$ is infinite if and only if there is an element $(x_1, \dots, x_t) \in P(A, B)$ such that*

$$(1.6) \quad \dim_{Z_i} \mathfrak{m}_{R_i}/\mathfrak{m}_{R_i}^2 \geq 2 \quad \text{and} \quad x_i \geq 2$$

for some $i \in \{1, \dots, t\}$.

- (2) *Suppose the orbit set $\mathcal{O}_{A,B}$ is finite, that is, for every element $(x_1, \dots, x_t) \in P(A, B)$, one has either $\dim_{Z_i} \mathfrak{m}_{R_i}/\mathfrak{m}_{R_i}^2 \leq 1$ or $x_i \leq 1$ for all $i \in \{1, \dots, t\}$. Then we have the formula*

$$|\mathcal{O}_{A,B}| = \sum_{(x_1, \dots, x_t) \in P(A,B)} \prod_{i=1}^t |\text{Mod}(\tilde{D}_i, x_i)|,$$

where $\text{Mod}(\tilde{D}_i, x_i)$ is the set of isomorphism classes of \tilde{D}_i -modules W with length $W = x_i$. The cardinality $|\text{Mod}(\tilde{D}_i, x_i)|$ is given by the following formula:

$$(1.7) \quad |\text{Mod}(\tilde{D}_i, x_i)| = \begin{cases} 1 & \text{if } x_i \leq 1, \\ p(x_i, e_i) & \text{if } x_i > 1 \text{ and } \dim_{Z_i} \mathfrak{m}_{R_i}/\mathfrak{m}_{R_i}^2 = 1 \end{cases}$$

where e_i is the smallest positive integer such that $\mathfrak{m}_{R_i}^{e_i} = 0$, and $p(x, e)$ denotes of number of all partitions $x = c_1 + \dots + c_s$ of x with each part $c_i \leq e$.

In the remaining part of this paper we give a few applications of main results. We analyze the problem of the local to global principle for the algebra embeddings over global fields. More precisely, let A be a central simple algebra over a global field F

and K a finite field extension of F with degree $k = [K : F]$ dividing $\deg(A)$, the degree of A . Can the problem of the embedding of K into A (i.e. $\text{Hom}_{F\text{-alg}}(K, A) \neq \emptyset$) be checked locally? It turns out that there are many examples so that the Hasse principle for embedding K in A does not hold. That is, the condition $\text{Hom}(K \otimes_F F_v, A \otimes_F F_v) \neq \emptyset$ for all places v may not imply that $\text{Hom}_{F\text{-alg}}(K, A) \neq \emptyset$.

Proposition 1.5. *Let K be any finite separable field extension of F of degree $k > 1$. Let $\delta = p_1^{n_1} \cdots p_r^{n_r}$ be a positive integer divisible by at least two primes, i.e. $r \geq 2$, with $k \mid \delta$. Assume that $k \leq \delta/p_i^{n_i}$ for all $i = 1, \dots, r$. Then there is a central division algebra Δ over F of degree δ such that the local-to-global principle for an embedding of K in Δ fails.*

See § 4.4 for the construction of such central division algebras Δ . This is the first example for the failure of the Hasse principle of embeddings fields in central simple algebras. Furthermore, we give a necessary and sufficient condition for a pair (K, A) so that the Hasse principle in question holds. We associate to each pair (K, A) an element

$$\bar{\mathbf{x}} = (\bar{\mathbf{x}}_w)_{w \in V^K} \in \bigoplus_{w \in V^K} \mathbb{Q}/\mathbb{Z}$$

as follows, where V^K and V^F denote the set of all places of K and F , respectively. Put

$$\mathbf{x}_w := \frac{c(A_v) \cdot \gcd(k_w, d_v)}{[K : F]} \in \mathbb{Q}_{>0}$$

and let $\bar{\mathbf{x}}_w$ be the class of \mathbf{x}_w in \mathbb{Q}/\mathbb{Z} , where

- $A_v := A \otimes_F F_v$ and $c(A_v)$ denotes the capacity of the central simple algebra A_v , where v is the place of F below w ,
- K_w is the completion of K at w and $k_w := [K_w : F_v]$, and
- d_v is the index of the algebra A_v .

Theorem 1.6. *Notations as above. Then there is an embedding of K into A over F if and only if there is an embedding of $K_v := K \otimes_F F_v$ into A_v over F_v for all $v \in V^F$ and the element $\bar{\mathbf{x}}$ vanishes.*

Theorem 1.6 states that the element $\bar{\mathbf{x}}$ is the only obstruction for the Hasse principle for an embedding of K in A . This can be used to study the Hasse principle for *families* of embeddings of fields in central simple algebras. For example, if $\delta = p^n$ for $n = 1, 2, 3$, where p is a prime number, then for any central simple algebra A of degree δ and any finite field extension K with $[K : F] \mid \delta$, then the Hasse principle in question for K and A holds. One can also show that this is optimal. That is, if δ is not of this form, then there exist a central simple algebra A of degree δ and a finite separable field extension K with $[K : F] \mid \delta$ such that the corresponding Hasse principle fails. We refer the reader to [9] for details.

Another applications are the determination of endomorphism algebras of abelian surfaces with quaternion algebras and the determination of characteristic polynomials of central simple algebras; see Section for details.

The paper is organized as follows. In Section 2 we determine when there is an algebra homomorphism between two given semi-simple algebras over a field in terms of numerical invariants. Section 3 treats the set of equivalence classes of

homomorphisms. We give a necessary and sufficient condition when this set is finite, and when this set is finite, we determine precisely its cardinality. In Section 4, we give a few applications of general results obtained in Sections 2 and 3.

2. THE EXISTENCE OF F -ALGEBRA HOMOMORPHISMS

2.1. Setting. Let F denote the ground field, which is arbitrary in this and next sections. All F -algebras in this paper are assumed to be finite-dimensional as F -vector spaces. As the standard convention, an F -algebra homomorphism between two F -algebras is a ring homomorphism over F , which particularly sends the identity to the identity. For the convenience of discussion, we introduce the following basic notion.

Definition 2.1. Let V be a finite-dimensional vector space over F , and A an (finite-dimensional) arbitrary F -algebra. We say that V is A -modulable if there is a right (or left) A -module structure on V . If B is any F -subalgebra of A and V is already a right (resp. left) B -module, then by saying V is A -modulable we mean that the right (resp. left) A -module structure on V is required to be compatible with the underlying B -module structure on V .

Theorem 2.2. Let A and B be two semi-simple F -algebras. We realize B as $\prod_{j=1}^r \text{End}_{\Delta_j}(V_j)$, where Δ_j is a division F -algebra and V_j is a right Δ_j -module for each j . Write $A = \prod_{i=1}^s A_i$ into simple factors as F -algebras.

- (1) The set $\text{Hom}_{F\text{-alg}}(A, B)$ is non-empty if and only if for each $j = 1, \dots, r$, there is a decomposition of V_j

$$V_j = V_{j1} \oplus \dots \oplus V_{js}$$

into Δ_j -subspaces such that the Δ_j -vector space V_{ji} is $\Delta_j \otimes_F A_i^o$ -modulable for $i = 1, \dots, s$, where A_i^o denotes the opposite algebra of A_i .

- (2) The set $\text{Hom}_{F\text{-alg}}^*(A, B)$ is non-empty if and only if in addition each direct sum $\oplus_{j=1}^r V_{ji}$ is non-zero for $i = 1, \dots, s$.

PROOF. Suppose we have a homomorphism $\varphi : A \rightarrow B$ of F -algebras, then we have a Δ_j -linear action of A on V_j for each $j = 1, \dots, r$. The decomposition $A = \prod_{i=1}^s A_i$ gives a decomposition of V_j

$$V_j = V_{j1} \oplus \dots \oplus V_{js},$$

where each V_{ji} is a (A_i, Δ_j) -bimodule or a right $\Delta_j \otimes_F A_i^o$ -module. If φ is an embedding, then for each i at least one of V_{ji} for $j = 1, \dots, r$ is non-zero. Therefore, the direct sum $\oplus_j V_{ji}$ is non-zero. Conversely, suppose that we are given such a decomposition with these properties. Then we have a Δ_j -linear action of A on each vector space V_j ; this gives an F -algebra homomorphism $\varphi : A \rightarrow B$. Moreover, suppose that each direct sum $\oplus_{j=1}^r V_{ji}$ is non-zero. Then the map restricted to A_i is injective for each i . Therefore, φ is an embedding. This proves the theorem. ■

2.2. Tensor products of two semi-simple algebras. According to Theorem 2.2 we shall need to determine whether a vector space is $A \otimes_F B$ -modulable for semi-simple algebras A and B . When A and B are separable F -algebras, the tensor product $A \otimes_F B$ is again separable [7, 7.19 Corollary, p. 101]. However, the tensor product $A \otimes_F B$ of two semi-simple algebras A and B needs not to be semi-simple.

The structure of $A \otimes_F B$ seems not be well-studied in the literature when both A and B are not separable F -algebras.

Proposition 2.3. *Let A and B be two semi-simple F -algebras. Let*

$$(A \otimes_F B)^{ss} \simeq \prod_{i=1}^t \text{Mat}_{m_i}(D_i)$$

be the Wedderburn decomposition of the maximal semi-simple quotient $(A \otimes_F B)^{ss}$. Then the F -algebra $A \otimes_F B$ is isomorphic to $\prod_{i=1}^t \text{Mat}_{m_i}(\tilde{D}_i)$ for some Artinian F -algebras \tilde{D}_i with $(\tilde{D}_i)^{ss} = D_i$.

PROOF. Write $A = \prod_i A_i$ and $B = \prod_j B_j$ into simple factors. Then $A \otimes_F B \simeq \prod_{i,j} A_i \otimes_F B_j$. Therefore, without loss of generality we may assume that A and B are simple. Let K and Z be the center of A and B , respectively. Since $K \otimes_F Z$ is a commutative Artinian F -algebra, it is isomorphic to the product $\prod_{i=1}^t R_i$ of some local Artinian F -algebra R_i . Each R_i is a both K -algebra and Z -algebra. We have

$$(2.1) \quad A \otimes_F B \simeq A \otimes_K (K \otimes_F Z) \otimes_Z B \simeq \prod_{i=1}^t A \otimes_K R_i \otimes_Z B.$$

Let R be one of R_i , and let \mathfrak{m} be the maximal ideal of R and $Z' := R/\mathfrak{m} = (R)^{ss}$ be the residue field. Put $\mathcal{C} := A \otimes_K R \otimes_Z B$. Since A and B are respective central simple K and Z -algebras, the map $I \mapsto A \otimes I \otimes B$ gives a bijection between the set of (2-sided) ideals of R and that of \mathcal{C} . In particular, $\text{rad}(\mathcal{C}) = A \otimes \mathfrak{m} \otimes B$. Put $\overline{\mathcal{C}} := \mathcal{C}/\text{rad}(\mathcal{C})$. One has

$$\overline{\mathcal{C}} := A \otimes_K Z' \otimes_Z B = \text{Mat}_m(D),$$

where D is a central division Z' -algebra.

Let $\{\epsilon_{ij}\} \subset \overline{\mathcal{C}}$ be the standard basis for $\text{Mat}_m(D)$ over D ; one has $\epsilon_{ij}\epsilon_{kl} = \delta_{jk}\epsilon_{il}$ for $1 \leq i, j, k, l \leq m$. By [7, (6.19) Theorem, p. 86], there exist orthogonal idempotents $e_{11}, \dots, e_{mm} \in \mathcal{C}$ such that $\bar{e}_{ii} = \epsilon_{ii}$ for all i and $1 = e_{11} + \dots + e_{mm}$. For $i = 1, \dots, m-1$, choose an element $e_{i,i+1} \in e_{ii}\mathcal{C}e_{i+1,i+1}$ with $\bar{e}_{i,i+1} = \epsilon_{i,i+1}$. The right multiplication by $e_{i,i+1}$ (denoted by $e_{i,i+1}$ again) is a lift of the right multiplication by $\epsilon_{i,i+1} : \overline{\mathcal{C}}\epsilon_{ii} \simeq \overline{\mathcal{C}}\epsilon_{i+1,i+1}$. By [7, (6.18) Theorem, p. 85], the map

$$e_{i,i+1} : \mathcal{C}e_{ii} \simeq \mathcal{C}e_{i+1,i+1}$$

is a \mathcal{C} -linear isomorphism. Let $e_{i+1,i} \in e_{i+1,i+1}\mathcal{C}e_{ii}$ be an element such that the right multiplication by $e_{i+1,i}$ is the inverse map of the map $e_{i,i+1} : \mathcal{C}e_{ii} \rightarrow \mathcal{C}e_{i+1,i+1}$. One thus has $e_{i,i+1}e_{i+1,i} = e_{ii}$ and $e_{i+1,i}e_{i,i+1} = e_{i+1,i+1}$. For $i < j$, define $e_{ij} := e_{i,i+1} \dots e_{j-1,j}$ and $e_{ji} := e_{j,j-1} \dots e_{i+1,i}$. Put $\tilde{D} := e_{11}\mathcal{C}e_{11}$. As a left \tilde{D} -module, \mathcal{C} is generated by $\{e_{ij}\}$ and it is easy to check that $e_{ij}\epsilon_{kl} = \delta_{jk}\epsilon_{il}$ for $1 \leq i, j, k, l \leq m$. This shows that $\mathcal{C} \simeq \text{Mat}_m(\tilde{D})$. This completes the proof of the proposition. ■

Lemma 2.4. *Let D be a division algebra over a field F and \tilde{D} be an Artinian F -algebra with maximal semi-simple quotient $(\tilde{D})^{ss} = D$. Then an F -vector space V is \tilde{D} -modulable if and only if*

$$[D : F] \mid \dim_F V.$$

PROOF. If V is a \tilde{D} -module, then there exists a filtration of \tilde{D} -submodules $V^i := (\text{rad}(\tilde{D}))^i V$. Each graded piece V^i/V^{i+1} is a D -module, and hence

$$[D : F] \mid \dim_F V^i/V^{i+1}.$$

Since $\dim_F V = \sum_i \dim_F V^i/V^{i+1}$, one has $[D : F] \mid \dim_F V$. Conversely, if V is a D -module, then it is also a \tilde{D} -module by the inflation. The condition $[D : F] \mid \dim_F V$ implies the a D -module structure on V exists. This completes the proof of the lemma. ■

Now we are ready to prove our first main theorem.

Theorem 2.5. *Let notations be as in Theorem 2.2.*

(1) *For each j , write the maximal semi-simple quotient*

$$(\Delta_j \otimes_F A^\circ)^{ss} = \prod_{k=1}^{t_j} \text{Mat}_{m_{jk}}(D_{jk})$$

of $\Delta_j \otimes_F A^\circ$ as the product of simple factors. Then the set $\text{Hom}_{F\text{-alg}}(A, B)$ is non-empty if and only if there are non-negative integers x_{jk} for $j = 1, \dots, r$ and $k = 1, \dots, t_j$ such that

- (a) $\sum_{k=1}^{t_j} x_{jk} = \dim_{\Delta_j} V_j$ for all j , and
- (b) for all j, k , one has

$$\frac{m_{jk}[D_{jk} : F]}{[\Delta_j : F]} \Big| x_{jk}.$$

(2) *For each j, i , write the maximal semi-simple quotient*

$$(\Delta_j \otimes_F A_i^\circ)^{ss} = \prod_{k=1}^{t_{ji}} \text{Mat}_{m_{jik}}(D_{jik})$$

of $\Delta_j \otimes_F A_i^\circ$ as the product of simple factors. Then the set $\text{Hom}_{F\text{-alg}}^(A, B)$ is non-empty if and only if there are non-negative integers x_{jik} for $j = 1, \dots, r$, $i = 1, \dots, s$ and $k = 1, \dots, t_{ji}$ such that*

- (a) $\sum_{i,k} x_{jik} = \dim_{\Delta_j} V_j$ for all j ,
- (b) for all j, i, k , one has

$$\frac{m_{jik}[D_{jik} : F]}{[\Delta_j : F]} \Big| x_{jik}, \quad \text{and}$$

(c) for all i , the sum $\sum_{j,k} x_{jik}$ is positive.

PROOF. (1) By Proposition 2.3, we have

$$(\Delta_j \otimes_F A^\circ) = \prod_{k=1}^{t_j} \text{Mat}_{m_{jk}}(\tilde{D}_{jk})$$

for some Artinian F -algebras \tilde{D}_{jk} with $(\tilde{D}_{jk})^{ss} = D_{jk}$. By Theorem 2.2, the set $\text{Hom}_{F\text{-alg}}(A, B)$ is non-empty if and only if V_j is $\Delta_j \otimes A^\circ$ -modulable for all j . In this case there is a decomposition of Δ_j -submodules of V_j ,

$$V_j = \bigoplus_{k=1}^{t_j} V_{jk},$$

such that each V_{jk} is $\text{Mat}_{m_{jk}}(\tilde{D}_{jk})$ -modulable. This is equivalent to, by Lemma 2.4, that $m_{jk}[D_{jk} : F] \mid \dim_F V_{jk}$. Put $x_{jk} := \dim_{\Delta_j} V_{jk}$. Then the integers x_{jk} satisfy the conditions (a) and (b).

(2) By Proposition 2.3, for each i and j we have

$$\Delta_j \otimes A_i^\circ = \prod_{k=1}^{t_{ji}} \text{Mat}_{m_{jik}}(\tilde{D}_{jik})$$

for some Artinian F -algebras \tilde{D}_{jik} with $(\tilde{D}_{jik})^{ss} = D_{jik}$. Then as in (1) for each j we have a decomposition $V_j = \oplus_{i,k} V_{jik}$ of Δ_j -submodules so that each V_{jik} is a $\text{Mat}_{m_{jik}}(\tilde{D}_{jik})$ -module and their sum $\oplus_k V_{jik}$ forms a right $\Delta_j \otimes A_i^\circ$ -module. Put $x_{jik} := \dim_{\Delta_j}(V_{jik})$. As in (1), the integers x_{jik} satisfy the conditions (a) and (b). Furthermore, a homomorphism $\varphi \in \text{Hom}_{F\text{-alg}}(A, B)$ is injective if and only if each simple factor A_i acts faithfully on the linear spaces $\{V_{jik}\}_{j,k}$. The latter is equivalent to the condition $\sum_{j,k} x_{jik} > 0$ for all $i = 1, \dots, s$. This proves the theorem. ■

2.3. Special cases. We apply the general theorem (Theorem 2.5) to the special case where B is a central simple F -algebra. Recall [7, p. 179, p. 253] the following definition for central simple algebras.

Definition 2.6. The *degree*, *capacity*, and *index* of a central simple algebra B over F are defined as

$$\deg(B) := \sqrt{[B : F]}, \quad c(B) := m, \quad i(B) := \sqrt{[\Delta : F]},$$

if $B \cong \text{Mat}_m(\Delta)$, where Δ is a division algebra over F , which is uniquely determined by B up to isomorphism. The algebra Δ is also called the *division part* of B .

Theorem 2.7. Let $B = \text{Mat}_n(\Delta)$ be a central simple algebra of F , where Δ is the division part of B . Let $A = \prod_{i=1}^s A_i$ be a semi-simple F -algebra and let K_i be the center of A_i for each i . Then there is an embedding of the F -algebra A into B if and only if there are positive integers n_i for $i = 1, \dots, s$ such that

$$(2.2) \quad n = \sum_{i=1}^s n_i, \quad \text{and} \quad [A_i : F] \mid n_i c_i, \quad \forall i = 1, \dots, s,$$

where c_i the capacity of the central simple algebra $\Delta \otimes_F A_i^\circ$ over K_i .

PROOF. Write

$$\Delta \otimes_F A_i^\circ = (\Delta \otimes_F K_i) \otimes_{K_i} A_i^\circ = \text{Mat}_{c_i}(D_i)$$

and we have

$$(2.3) \quad [\Delta : F][A_i : F] = c_i^2 [D_i : F].$$

By Theorem 2.5, there exists an embedding of the F -algebra A to B if and only if there are positive integers n_i for $i = 1, \dots, s$ such that $n = \sum_{i=1}^s n_i$ and

$$(2.4) \quad \frac{c_i [D_i : F]}{[\Delta : F]} \mid n_i, \quad \forall i = 1, \dots, s.$$

Using (2.3), the condition (2.4) is equivalent to $[A_i : F] \mid n_i c_i$. This proves the theorem. ■

We apply Theorem 2.7 to the case where the semi-simple algebra $A = K$ is commutative and obtain the following well-known result (cf. [6, Proposition 2.6] and [1, Section 4]).

Corollary 2.8. *Let $B = \text{Mat}_n(\Delta)$ be a central simple algebra over F and $K = \prod_{i=1}^s K_i$ is commutative semi-simple F -algebra. Assume that $[K : F] = \deg(B)$. Then there exists an embedding of K into A if and only if each K_i splits B .*

PROOF. By Theorem 2.7, the F -algebra K can be embedded into B if and only if there are positive integers n_i for $i = 1, \dots, s$ such that

$$(2.5) \quad n = \sum_{i=1}^s n_i, \quad \text{and} \quad [K_i : F] \mid n_i c_i, \quad \forall i = 1, \dots, s,$$

where $c_i = c(\Delta \otimes_F K_i)$. We need to show that $\deg(\Delta) = c_i$, i.e. K_i splits Δ for all i . Since $[K : F] = \deg(B)$, we have

$$[K : F] = \deg(B) = \sum_i n_i \deg(\Delta) \geq \sum_i n_i c_i \geq \sum_i [K_i : F] = [K : F].$$

It follows that $c_i = \deg(\Delta)$ for each i . ■

3. F -ALGEBRA HOMOMORPHISMS

In this section we shall find a necessary and sufficient condition for which the orbit set

$$(3.1) \quad \mathcal{O}_{A,B} := B^\times \backslash \text{Hom}_{F\text{-alg}}(A, B)$$

is finite, where A and B are given semi-simple F -algebras. Then we determine the cardinality $|\mathcal{O}_{A,B}|$ when it is finite.

If we write $B = \prod_{j=1}^r B_j$ into simple factors, then one has

$$(3.2) \quad \mathcal{O}_{A,B} = \prod_{j=1}^r \mathcal{O}_{A,B_j}.$$

Therefore, we may and do assume that B is simple. Write $B = \text{End}_\Delta(V)$, where Δ is a division algebra over F . Write

$$(3.3) \quad \Delta \otimes_F A^\circ \simeq \prod_{i=1}^t \text{Mat}_{m_i}(\tilde{D}_i)$$

as in Proposition 2.3 and put

$$(3.4) \quad D_i := (\tilde{D}_i)^{ss}, \quad R_i := Z(\tilde{D}_i), \quad Z_i := Z(D_i) = (R_i)^{ss}.$$

Since there is an embedding of Δ into $\text{Mat}_{m_i}(D_i)$, we have

$$[\Delta : F] \mid m_i [D_i : F].$$

Put

$$(3.5) \quad \ell_i := m_i [D_i : F] / [\Delta : F],$$

and

$$(3.6) \quad P(A, B) := \{(x_1, \dots, x_t) \in \mathbb{Z}_{\geq 0}^t \mid \dim_\Delta V = \sum_{i=1}^t \ell_i x_i\}.$$

By Theorem 2.5, the orbit set $\mathcal{O}_{A,B}$ is non-empty if and only if there is a decomposition $V = \oplus_i V_i$ of Δ -submodules such that

$$(3.7) \quad \dim_{\Delta} V_i = \ell_i x_i, \quad \text{for some non-negative integers } x_i.$$

or equivalently, the partition set $P(A, B)$ is non-empty.

Definition 3.1. Let D be a division algebra over F and \tilde{D} be an Artinian F -algebra with $\tilde{D}^{ss} = D$. For any non-negative integer n , denote by $\text{Mod}(\tilde{D}, n)$ the set of equivalent classes of \tilde{D} -modules W with length $W = n$.

Note that length $W = n$ if and only if $\dim_F W = n[D : F]$ (cf. Lemma 2.4).

Lemma 3.2. Let $\varphi_1, \varphi_2 \in \text{Hom}_{F\text{-alg}}(A, \text{End}_{\Delta}(V))$ be two maps. Let $W^{(i)}$ be the (A, Δ) -bimodule on V defined through φ_i for $i = 1, 2$. Then φ_1 and φ_2 are equivalent if and only if $W^{(1)}$ and $W^{(2)}$ are isomorphic as (A, Δ) -bimodules.

PROOF. If $W^{(1)}$ and $W^{(2)}$ are isomorphic, then there is a Δ -linear automorphism $g : V \rightarrow V$ such that the following diagram

$$\begin{array}{ccc} V & \xrightarrow{g} & V \\ \downarrow \varphi_1(a) & & \downarrow \varphi_2(a) \\ V & \xrightarrow{g} & V \end{array}$$

commutes for all $a \in A$. Therefore, $\varphi_2 = \text{Int}(g) \circ \varphi_1$. Conversely, if we are given g such that $\varphi_2 = \text{Int}(g) \circ \varphi_1$, then the map $g : V \rightarrow V$ is an (A, Δ) -linear isomorphism from $W^{(1)}$ to $W^{(2)}$. ■

Equivalently, the condition in Lemma 3.2 says that $W^{(1)}$ and $W^{(2)}$ are isomorphic as right $\Delta \otimes_F A^{\circ}$ -modules.

Using Lemma 3.2 and the discussion above we obtain the following result. Note following from (3.5) and (3.7) that V_i is a right $\text{Mat}_{m_i}(\tilde{D}_i)$ -module with

$$\dim_F V_i = [D_i : F] m_i x_i.$$

Using the Morita equivalence, the module $V_i = W_i^{\oplus m_i}$ determines uniquely an element $W_i \in \text{Mod}(\tilde{D}_i, x_i)$.

Theorem 3.3. Notations being as above. There is a bijection between the orbit set $\mathcal{O}_{A,B}$ and

$$(3.8) \quad \coprod_{(x_1, \dots, x_t) \in P(A, B)} \prod_{i=1}^t \text{Mod}(\tilde{D}_i, x_i).$$

Theorem 3.3 tells us that

- (1) the orbit set $\mathcal{O}_{A,B}$ is non-empty if and only if so is the set $P(A, B)$;
- (2) the orbit set $\mathcal{O}_{A,B}$ is finite if and only if each set $\text{Mod}(\tilde{D}_i, x_i)$ is finite for all $i = 1, \dots, t$ and for all $(x_1, \dots, x_t) \in P(A, B)$;
- (3) if $\mathcal{O}_{A,B}$ is finite, then

$$(3.9) \quad |\mathcal{O}_{A,B}| = \sum_{(x_1, \dots, x_t) \in P(A, B)} \prod_{i=1}^t |\text{Mod}(\tilde{D}_i, x_i)|.$$

It remains to determine when a set of the form $\text{Mod}(\tilde{D}, x)$ is finite, and to compute its cardinality $|\text{Mod}(\tilde{D}, x)|$ if it is so. By definition, one has $|\text{Mod}(\tilde{D}, 0)| = 1$.

Proposition 3.4. *Let D be a division algebra over F , and let \tilde{D} be an Artinian F -algebra with $(\tilde{D})^{ss} = D$. Let $R := Z(\tilde{D})$ and $Z := R/\mathfrak{m}_R$ be the residue field of R .*

- (1) *The set $\text{Mod}(\tilde{D}, 1)$ is finite and $|\text{Mod}(\tilde{D}, 1)| = 1$.*
- (2) *If the ground field F is finite, then the set $\text{Mod}(\tilde{D}, x)$ is finite.*
- (3) *If $\mathfrak{m}_R = 0$, then $\tilde{D} = D$ and $|\text{Mod}(\tilde{D}, x)| = 1$.*
- (4) *Suppose $\dim_Z \mathfrak{m}_R/\mathfrak{m}_R^2 = 1$. Let e be the smallest positive integer such that $\mathfrak{m}_R^e = 0$. Then for any positive integer x , the set $\text{Mod}(\tilde{D}, x)$ is finite and $|\text{Mod}(\tilde{D}, x)|$ is equal to the number $p(x, e)$ of partitions $x = c_1 + \cdots + c_r$, for some $r \in \mathbb{N}$, of x with each part $1 \leq c_i \leq e$.*

PROOF. (1) It is clear. (2) This follows from the finiteness of

$$\text{Hom}_{F\text{-alg}}(\tilde{D}, \text{Mat}_c(F)) \subset \text{Hom}_{F\text{-lin}}(\tilde{D}, \text{Mat}_c(F)) = \text{Mat}_{\dim \tilde{D} \times c^2}(F),$$

where $c := [D : F]x$. (3) It is clear.

(4) Choose a generator $\pi \in \mathfrak{m}_R$ so that $\pi \in R \in \tilde{D}$, $\pi^e = 0$ and $\tilde{D}/\pi\tilde{D} = D$. Every finite \tilde{D} -module is isomorphic to

$$\tilde{D}/(\pi^{c_1}) \oplus \tilde{D}/(\pi^{c_2}) \oplus \cdots \oplus \tilde{D}/(\pi^{c_r}), \quad \text{for some } r \in \mathbb{N},$$

where $1 \leq c_1 \leq \cdots \leq c_r$ are integers with each $c_i \leq e$. The proof is similar to that for the classification of finite $F[\pi]/(\pi^e)$ -modules. We leave the details to the reader. This completes the proof of the proposition. ■

Proposition 3.5. *Let \tilde{D} , D , R , Z , and \mathfrak{m}_R be as in Proposition 3.4. If*

- (i) $\dim_Z \mathfrak{m}_R/\mathfrak{m}_R^2 \geq 2$,
- (ii) *the ground field F is infinite, and*
- (iii) *the integer $x \geq 2$,*

then the set $\text{Mod}(\tilde{D}, x)$ is infinite.

PROOF. By Cohen's theorem, one can write

$$R \simeq Z[x_1, \dots, x_n] = Z[X_1, \dots, X_n]/(f_j(X))_j, \quad n \geq 2,$$

with every equation $f_j(X) \in (X_1, \dots, X_n)^2$. Then R admits a quotient

$$R_1 \simeq Z[x_1, x_2] = Z[X_1, X_2]/(X_1^2, X_1X_2, X_2^2).$$

Put $\tilde{D}_1 := \tilde{D} \otimes_R R_1$, which is a quotient of \tilde{D} . The inflation operation gives the inclusion map $\text{Mod}(\tilde{D}_1, x) \subset \text{Mod}(\tilde{D}, x)$. Therefore, it suffices to show that the set $\text{Mod}(\tilde{D}_1, x)$ is infinite. We shall construct infinitely many non-isomorphic \tilde{D}_1 -modules M in $\text{Mod}(\tilde{D}_1, x)$. View D as a \tilde{D}_1 -module by inflation. For any element $a \in F$, put

$$M_a := \tilde{D}_1/(x_1 + ax_2) \oplus D^{\oplus x-2}.$$

It is clear that $\dim_F M_a = [D : F]x$ and that the annihilator $\text{Ann}(M_a) = \tilde{D}_1(x_1 + ax_2)$. For $a, b \in F$, if $M_a \simeq M_b$ then $\text{Ann}(M_a) = \text{Ann}(M_b)$ and hence $a = b$. This shows that if F is infinite then there are infinitely many non-isomorphic \tilde{D}_1 -modules in $\text{Mod}(\tilde{D}_1, x)$. ■

We refine our main theorem (Theorem 3.3) by Propositions 3.4 and 3.5 as follows.

Theorem 3.6. *Let A be a semi-simple F -algebra and B a simple F -algebra. Let $\tilde{D}_i, D_i, R_i, Z_i$ and $P(A, B)$ be as above.*

- (1) *The orbit set $\mathcal{O}_{A,B}$ is infinite if and only if there is an element $(x_1, \dots, x_t) \in P(A, B)$ such that*

$$(3.10) \quad \dim_{Z_i} \mathfrak{m}_{R_i} / \mathfrak{m}_{R_i}^2 \geq 2 \quad \text{and} \quad x_i \geq 2$$

for some $i \in \{1, \dots, t\}$.

- (2) *Suppose the orbit set $\mathcal{O}_{A,B}$ is finite, that is, for every element $(x_1, \dots, x_t) \in P(A, B)$, one has either $\dim_{Z_i} \mathfrak{m}_{R_i} / \mathfrak{m}_{R_i}^2 \leq 1$ or $x_i \leq 1$ for all $i \in \{1, \dots, t\}$. Then*

$$|\mathcal{O}_{A,B}| = \sum_{(x_1, \dots, x_t) \in P(A,B)} \prod_{i=1}^t |\text{Mod}(\tilde{D}_i, x_i)|.$$

Moreover,

$$(3.11) \quad |\text{Mod}(\tilde{D}_i, x_i)| = \begin{cases} 1 & \text{if } x_i \leq 1, \\ p(x_i, e_i) & \text{if } x_i > 1 \text{ and } \dim_{Z_i} \mathfrak{m}_{R_i} / \mathfrak{m}_{R_i}^2 = 1 \end{cases}$$

where e_i is the smallest positive integer such that $\mathfrak{m}_{R_i}^{e_i} = 0$, and $p(x, e)$ denotes of number of all partitions $x = c_1 + \dots + c_s$ of x with each part $c_i \leq e$.

Note that the condition $\dim_{Z_i} \mathfrak{m}_{R_i} / \mathfrak{m}_{R_i}^2 \geq 2$ in (3.10) can occur only when F is infinite. The general case where B is semi-simple can be reduced to the simple case as Theorem 3.6 by (3.2).

As an immediate consequence of Theorem 3.6, the following result improves the main results of F. Pop and H. Pop in [5].

Corollary 3.7. *Let A and B be semi-simple F -algebras. Assume that A or B is separable over F . Then the orbit set $\mathcal{O}_{A,B}$ is finite and $|\mathcal{O}_{A,B}| = |P(A, B)|$.*

We have defined the set $P(A, B)$ when B is simple. When B is semi-simple, if we write $B = \prod_{j=1}^r B_j$ into simple factors, then the set $P(A, B)$ is defined as

$$P(A, B) := \prod_{j=1}^r P(A, B_j).$$

4. SOME APPLICATIONS

In this section, we give a few applications of the results in the previous sections.

4.1. Characteristic polynomials of central simple algebras. Let A be a (f.d.) central simple algebra over an arbitrary base field F . Let $A = \text{End}_\Delta(V) = \text{End}_n(\Delta)$, where Δ is a central division algebra over F , V is a right Δ -vector space of dimension. For any element $x \in A = \text{Mat}_n(\Delta)$, the *characteristic polynomial of x* is defined to be the characteristic polynomial of the image of x in $\text{Mat}_{nd}(\bar{F})$ under a map

$$A \rightarrow A \otimes_F \bar{F} \xrightarrow{\rho} \text{Mat}_{nd}(\bar{F}),$$

where \bar{F} is an algebraic closure of F and d is the degree of Δ . This polynomial is independent of the choice of the isomorphism ρ and it is defined over F . We

call a monic polynomial of degree nd is a characteristic polynomial of A if it is the characteristic polynomial of some element in A . A natural question is to determine whether a given polynomial is a characteristic polynomial of A . We have the following result.

Theorem 4.1. *Let $f(t) \in F[t]$ be a monic polynomial of degree nd and let $f(t) = \prod_{i=1}^s p_i(t)^{a_i}$ be the factorization into irreducible polynomials. Put $F_i := F[t]/(p_i(t))$. Then $f(t)$ is a characteristic polynomial of A if and only if for all $i = 1, \dots, s$, one has*

- (a) $a_i \deg p_i(t) = n_i d$ for some positive integer n_i , and
- (b) $[F_i : F] \mid n_i \cdot c(\Delta \otimes_F F_i)$.

The idea of the proof is to reduce first the case where $f(t)$ is a power of an irreducible polynomial. More precisely, one can show that $f(t)$ is a characteristic polynomial if and only if

- (a) $a_i \deg p_i(t) = n_i d$ for some positive integer n_i , and
- (c) each $p_i(t)^{a_i}$ is a characteristic polynomial of $\text{Mat}_{n_i}(\Delta)$.

Then one can show that the condition (c) is equivalent to that the field extension F_i can be embedded into $\text{Mat}_{n_i}(\Delta)$. Then we use Theorem 2.7 to show that this is equivalent to (b). The details can be found in [11].

We remark that when F is a non-Archimedean local field, the condition (b) can be replaced by the following simpler condition

- (d) $\deg p_i(t) \mid n_i \gcd(d, \deg p_i(t))$.

This follows from the formula $\text{inv}_{F_i}(\Delta \otimes_F F_i) = \text{inv}_F(\Delta)[F_i : F]$, where $\text{inv}_F(\Delta)$ is the invariant of Δ .

4.2. Endomorphism algebras of QM abelian surfaces. We can apply the embedding result to determine all possible endomorphism algebras of abelian surfaces with quaternion multiplication (QM). Let D be an indefinite quaternion division algebra over the field \mathbb{Q} of rational numbers. It is interesting to find out all \mathbb{Q} -algebras E containing D which appear as endomorphism algebras of abelian surfaces. In other words, we would like to know which endomorphism algebra appears in the Shimura curve X_D associated to the quaternion algebra D (and with additional data). Studying whether or not a semi-simple algebras over \mathbb{Q} can appear as the endomorphism algebra of an abelian variety is a way to understand structures of abelian varieties. See Oort [3] for detail discussions and extensive information for this problem.

Theorem 4.2. *Let D be an indefinite quaternion division algebra over \mathbb{Q} , and let A be an abelian surface over a field k with quaternion multiplication by D , i.e. an abelian surface together with a \mathbb{Q} -algebra embedding $\iota : D \rightarrow E := \text{End}^0(A) := \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

- (1) *Suppose that A is not simple. Then A is isogenous to C^2 for an elliptic curve C and the algebra E is isomorphic to one of the following*
 - (i) $\text{Mat}_2(K)$, where K is any imaginary quadratic field which splits D , or
 - (ii) $\text{Mat}_2(D_{p,\infty})$, where $D_{p,\infty}$ is the quaternion algebra over \mathbb{Q} ramified exactly at $\{p, \infty\}$. This occurs if and only if C is a supersingular elliptic curve over the base field $k \supset \mathbb{F}_{p^2}$.
- (2) *Suppose that A is simple. Then*

- (i) $E \simeq D$, or
- (ii) $E \simeq D_K := D \otimes_{\mathbb{Q}} K$ for some imaginary quadratic field K . In this case, the abelian surface A is in characteristic $p > 0$ for some prime p and it is supersingular.

The algebra D (the case (2) (i)) can occur as we can take a generic complex abelian surface with QM by D . Recall that an abelian variety in characteristic $p > 0$ is said to be *supersingular* if it is isogenous to a product of supersingular elliptic curves over a finite field extension. The case (ii) of Theorem 1.1 (2) can occur only when the quaternion algebra D satisfies certain conditions. In this case, the algebra E is determined by its center K , and there are only a finite list of possibilities for such K . More precisely, we have the following result.

Theorem 4.3. *Let A be a simple supersingular abelian surface over a finite field \mathbb{F}_q of characteristic $p > 0$ with quaternion multiplication by D . Let $E := \text{End}^0(A)$ and S be the discriminant of D . Then*

- (1) *The center K of E is isomorphic to $\mathbb{Q}(\zeta_n)$ for $n = 3, 4$, or 6 .*
- (2) *$p \mid S$ and $p \equiv 1 \pmod{n}$, where n is as above, and for any other prime $\ell \mid S$, one has either $\ell \mid n$ or $\ell \equiv -1 \pmod{n}$, that is, ℓ does not split in the quadratic field $\mathbb{Q}(\zeta_n)$.*
- (3) *$E \simeq D \otimes_{\mathbb{Q}} K$.*

Theorem 4.3 states that there are three possibilities for endomorphism algebras E of simple supersingular abelian surfaces over finite fields: $E \simeq D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_n)$ for $n = 3, 4, 6$. However, not all of them occur; it depends on the quaternion algebra D . The algebra $D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_n)$ occurs if and only if there is exactly one prime $p \mid S$ such that $p \equiv 1 \pmod{n}$.

These results contribute (Theorems 4.2 and 4.3) new cases to the problem of semi-simple algebras appearing as endomorphism algebras of abelian varieties as mentioned above (see Oort [3]). The proofs and details will be published elsewhere.

In the last part of this section, we add some details to the local-global principle for embeddings of fields in simple algebras in Section 1.

4.3. Embeddings over global fields. We let the base field F be a global field. Let A be a central simple algebra over F and let K be a finite field extension of F with $k := [K : F] \mid \deg(A)$. Consider the local-global principle for embeddings of K in A . That is, if there exists an embedding of $K_v := K \otimes_F F_v$ in $A_v := A \otimes_F F_v$ for all places $v \in V^F$, does there exist an embedding of K in A ? When K has the maximal degree, the answer is yes and this is a useful result.

We use the following notations

- $A = \text{End}_{\Delta}(V)$, where Δ is the division part of A , and V is a finite right Δ -module of rank n .
- $k := [K : F]$ and $\delta := \deg(\Delta)$.
- For any place v of F , denote by F_v the completion of F at v . Put

$$K_v := K \otimes F_v = \prod_{w|v} K_w, \quad A_v := A \otimes F_v, \quad \Delta_v = \Delta \otimes F_v = \text{Mat}_{s_v}(D_v),$$

where D_v is the division part of the central simple algebra Δ_v and s_v is the capacity of Δ_v .

- $k_w := [K_w : F_v]$ and $d_v := \deg(D_v)$, where w is a place of K over v .
- $\Delta \otimes_F K = \text{Mat}_c(\Delta')$ and $\delta' := \deg(\Delta')$, where Δ' is the division part of the central simple algebra $\Delta \otimes K$ over K , and c is its capacity. One has

$$(4.1) \quad \delta = \delta' c.$$

- For any place w of K , put

$$\Delta'_w := \Delta' \otimes_K K_w = \text{Mat}_{t_w}(D'_w), \quad d'_w := \deg(D'_w),$$

where D'_w is the division part of the central simple algebra Δ'_w and t_w is the local capacity of Δ' at w .

- $c_w := c(D_v \otimes_{F_v} K_w)$, i.e. $D_v \otimes_{F_v} K_w = \text{Mat}_{c_w}(D'_w)$. One has

$$(4.2) \quad d_v = d'_w c_w.$$

It follows from $\text{inv}(D'_w) = \text{inv}(D_v)[K_w : F_v]$ (see [8]) that

$$(4.3) \quad c_w = (d_v, k_w).$$

- For each place v of F , write

$$\text{inv}_v(\Delta) = \frac{a_v}{\delta} = \frac{a'_v s_v}{d_v s_v} = \frac{a'_v}{d_v}, \quad (a'_v, d_v) = 1 \text{ and } s_v = (a_v, \delta).$$

One has, by the Grunwald-Wang theorem

$$(4.4) \quad \delta = \text{lcm}\{d_v\}_{v \in V^F} \quad \text{and} \quad (\gcd\{a_v\}_{v \in V^F}, \delta) = 1,$$

where V^F denotes the set of all places of F .

- For each place w of K , write

$$\text{inv}_w(\Delta') = \frac{b_w}{\delta'} = \frac{b'_w t_w}{d'_w t_w} = \frac{b'_w}{d'_w}, \quad (b'_w, d'_w) = 1 \text{ and } t_w = (b_w, \delta').$$

One has

$$(4.5) \quad \delta' = \text{lcm}\{d'_w\}_{w \in V^K} \quad \text{and} \quad (\gcd\{b_w\}_{w \in V^K}, \delta') = 1,$$

where V^K denotes the set of all places of K .

Given K and A , we have, for each place v of F ,

- a tuple $(k_w)_{w|v}$ of positive integers, and
- a rational number $\text{inv}_v(\Delta) = a'_v/d_v$

satisfying the following conditions:

- $\sum_{w|v} k_w = k$ for all $v \in V^F$,
- $d_v = 1$ if v is a complex place,
 - $d_v \in \{1, 2\}$ if v is a real place,
 - $d_v = 1$ for almost all v , and
 - (Global class field theory) one has

$$\sum_{v \in V^F} \frac{a'_v}{d_v} = 0.$$

We compute all other numerical invariants δ , c_w , d'_w , δ' and c as follows.

- The (global) degree δ of Δ can be computed by (4.4).
- Then one computes the local capacity c_w of $D_v \otimes_{F_v} K_w$ and the (local) degree d'_w of D'_w by (4.3) and (4.2), respectively.

- (iii) Using (4.5) we compute the (global) degree δ' of Δ' and then compute the (global) capacity c of $\Delta \otimes K$ using (4.1).

Theorem 2.7 states that $\text{Hom}_F(K, A) \neq \emptyset$ if and only if $k \mid nc$. This provides a simple numerical criterion how to check when there is an embedding $K \hookrightarrow A$.

Now we analyze the obstruction to the corresponding local-global principle. Similar to (3.6) we define for each $v \in V^F$ a finite set

$$(4.6) \quad \mathcal{E}_v := \mathcal{E}_{F_v}(K_v, A_v) = \{(x_w)_{w|v} \mid x_w \in \mathbb{N}, \sum_{w|v} \ell_w x_w = ns_v\},$$

where $\ell_w := k_w/c_w$.

Theorem 3.3 (also with Theorem 2.5 (2)) states that there is an isomorphism

$$e_v : A_v^\times \setminus \text{Hom}_{F_v}^*(K_v, A_v) \xrightarrow{\sim} \mathcal{E}_v.$$

If $\varphi_v \in \text{Hom}_{F_v}^*(K_v, A_v)$, then it gives to a decomposition of *non-zero* D_v -submodules V_w

$$D_v^{ns_v} = \bigoplus_{w|v} V_w, \quad \dim_{D_v} V_w = n_w$$

with the property $k_w \mid n_w c_w$ or equivalently $\ell_w \mid n_w$. Then $e_v([\varphi_v])$ is given by the formula

$$(4.7) \quad e_v([\varphi_v]) = \left(\frac{n_w}{\ell_w} \right)_{w|v}.$$

Let us suppose first that the set $\text{Hom}_F(K, A)$ of embeddings from K into A over F is *non-empty*. For any element φ in $\text{Hom}_F(K, A)$, let $\varphi_v \in \text{Hom}_{F_v}(K_v, A_v)$ be the extension of φ by F_v -linearity, and let $[\varphi_v]$ be its equivalence class. Then one gets an element $\mathbf{x}_v \in \mathcal{E}_v$ by

$$\mathbf{x}_v := e_v([\varphi_v]) = (\mathbf{x}_w)_{w|v}.$$

Simple computation shows that

$$(4.8) \quad \mathbf{x}_w := \dim_{D_v} W_w / \ell_w = ns_v c_w / k,$$

which is a positive integer.

Without knowing $\text{Hom}_F(K, A)$ is non-empty, we still define an element $\mathbf{x}_w \in \mathbb{Q}$ for each $w \in V^K$ by (4.8). Let $\bar{\mathbf{x}}_w$ be the image of \mathbf{x}_w in \mathbb{Q}/\mathbb{Z} . We associate to the pair (K, A) an element

$$\bar{\mathbf{x}} := (\bar{\mathbf{x}}_w)_{w \in V^K} \in \bigoplus_{w \in V^K} \mathbb{Q}/\mathbb{Z}.$$

The vanishing of the class $\bar{\mathbf{x}}$ is an obstruction for the set $\text{Hom}_F(K, A)$ be non-empty. Moreover, the following result states that this is the only obstruction.

Theorem 4.4. *Notations as above. We have*

$$\text{Hom}_F^*(K, A) \neq \emptyset \iff \bar{\mathbf{x}} = 0.$$

PROOF. See [9, Theorem 3.6]. ■

4.4. Construction of examples. For a central simple algebra A over a global field F and a finite field extension K over F , we say that the Hasse principle for the pair (K, A) holds if one has the equivalence of the conditions

$$\mathrm{Hom}_F^*(K, A) \neq \emptyset \iff \mathrm{Hom}_{F_v}^*(K_v, A_v) \neq \emptyset, \quad \forall v \in V^F.$$

In this subsection we shall construct a family of examples (K, A) so that the Hasse principle for (K, A) fails.

Lemma 4.5. *Let S be a finite set of places of a global field F . Let L_v , for each $v \in S$, be any étale F_v -algebra of the same degree $[L_v : F_v] = d$. Then there exists a finite separable field extension K of F of degree d such that $K \otimes_F F_v \simeq L_v$ for all $v \in S$.*

PROOF. This follows from the Hilbert irreducibility theorem and Krasner's lemma; also see a proof in [10, Lemma 3.2]. ■

Let K be any finite separable field extension of F of degree $k = [K : F] > 1$, and let δ be a positive integer with more than one prime divisors and divisible by k . Write $\delta = p_1^{n_1} \dots p_r^{n_r}$, $r \geq 2$ and $n_i \geq 1$, where each p_i is a prime number.

Assume that $k \leq \delta/p_i^{n_i}$ for all i . We claim that there is a central division algebra Δ over F of degree δ so that the Hasse principle for the pair (K, Δ) fails.

Choose $2r$ places $v_1, v'_1, \dots, v_r, v'_r$ of F which split completely in K . One has

$$K_{v_i} = \prod_{j=1}^k K_{w_{ij}}, \quad K_{w_{ij}} \simeq F_{v_i}, \quad \text{and} \quad K_{v'_i} = \prod_{j=1}^k K_{w'_{ij}}, \quad K_{w'_{ij}} \simeq F_{v'_i}, \quad \forall i.$$

Choose a central division algebra Δ over F with following local invariants:

- $\mathrm{inv}_{v_i}(\Delta) = -\mathrm{inv}_{v'_i}(\Delta) = 1/p_i^{n_i}$ for $i = 1, \dots, r$, and
- $\mathrm{inv}_v(\Delta) = 0$ for other places v .

Then Δ has degree δ . For all i , we have

$$(4.10) \quad s_{v_i} = s_{v'_i} = \delta/p_i^{n_i}, \quad c_{w_{ij}} = 1, \quad \mathbf{x}_{w_{ij}} = s_{v_i}/k, \quad \ell_{w_{ij}} = 1,$$

and

$$\mathcal{E}_{v_i} \simeq \mathcal{E}_{v'_i} = \left\{ (x_j) \in \mathbb{N}^k; \sum_{j=1}^k x_j = s_{v_i} \right\}.$$

Since $k \leq s_{v_i}$, the sets \mathcal{E}_{v_i} and $\mathcal{E}_{v'_i}$ are non-empty; the remaining sets \mathcal{E}_v for unramified places v are also non-empty due to $k \mid \delta$.

Suppose that the Hasse principle for (K, Δ) holds, then one has $\mathbf{x}_{w_{ij}} \in \mathbb{N}$ for all i by Theorem 4.4. This implies that $k = 1$ as $\gcd\{s_{v_i}\}_i = 1$, a contradiction.

ACKNOWLEDGMENTS

Part of this work was done during the author's stays at Tsinghua University in Beijing and at Universität Duisburg-Essen. He wishes to thank Linsheng Yin and U. Görtz for their kind invitation and hospitality. The author was partially supported by grants NSC 97-2115-M-001-015-MY3 and AS-99-CDA-M01.

REFERENCES

- [1] P. Chuard-Koulmann and J. Morales, Extending involutions on Frobenius algebras. *Manuscripta Math.* **108** (2002), 439–451.
- [2] H. Matsumura, *Commutative algebra*. Second edition. Mathematics Lecture Note Series, 56. Benjamin/Cummings Publishing, 1980, 313 pp.
- [3] F. Oort, Endomorphism algebras of abelian varieties. *Algebraic geometry and commutative algebra, in honor of M. Nagata* (1988), 469–502.
- [4] R. S. Pierce, *Associative algebras*. Graduate Texts in Mathematics, **88**. Springer-Verlag, New York-Berlin, 1982. 436 pp.
- [5] F. Pop and H. Pop, An extension of the Noether-Skolem theorem. *J. Pure Appl. Algebra* **35** (1985), no. 3, 321–328.
- [6] G. Prasad and A. Rapinchuk, Local-global principles for embedding of fields with involution into simple algebras with involution, *Comment. Math. Helv.* **85** (2010), 583–645.
- [7] I. Reiner, *Maximal orders*. London Mathematical Society Monographs, No. **5**. Academic Press, London-New York, 1975, 395 pp.
- [8] J.-P. Serre, *Local fields*. **GTM 67**, Springer-Verlag, 1979.
- [9] Sheng-Chi Shih, Tse-Chung Yang and C.-F. Yu, Embeddings of fields in simple algebras over global fields. arXiv:1108.0830. 27 pp.
- [10] C.-F. Yu, Construction of Galois covers of curves with groups of SL_2 -type. *C. R. Acad. Sci. Paris Sér. I Math.* **345** (2007), 77–80.
- [11] C.-F. Yu, Characteristic polynomials of central simple algebras. arXiv:1109.3851, 7 pp.

INSTITUTE OF MATHEMATICS, ACADEMIA SINICA AND NCTS (TAIPEI OFFICE), 6TH FLOOR,
 ASTRONOMY MATHEMATICS BUILDING, NO. 1, ROOSEVELT RD. SEC. 4, TAIPEI, TAIWAN, 10617
E-mail address: chiafu@math.sinica.edu.tw